



The New York Times | <http://nyti.ms/1I12OLG>

EUROPE | TECHNOLOGY

Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Paris Attacks

By **DAVID E. SANGER** and **NICOLE PERLROTH** NOV. 16, 2015

WASHINGTON — American and French officials say there is still no definitive evidence to back up their presumption that the terrorists who massacred 129 people in Paris used new, difficult-to-crack encryption technologies to organize the plot.

But in interviews, Obama administration officials say the Islamic State has used a range of encryption technologies over the past year and a half, many of which defy cracking by the National Security Agency. Other encryption technologies, the officials hint, are less secure than terrorist and criminal groups may believe, and clearly they want to keep those adversaries guessing which ones the N.S.A. has pierced.

Some of the most powerful technologies are free, easily available encryption apps with names like Signal, Wickr and Telegram, which encode mobile messages from cellphones. Islamic State militants used Telegram two weeks ago to claim responsibility for the crash of the Russian jet in the Sinai Peninsula that killed 224 people, and used it again last week, in Arabic, English and French, to broadcast responsibility for the Paris carnage. It is not yet clear whether they also used

Telegram's secret-messaging service to encrypt their private conversations.

Nonetheless, such "end-to-end" encryption technology is now so widespread that the attack has revived vitriolic arguments between American intelligence officials and Silicon Valley. Only weeks ago, the matter appeared settled, at least temporarily, with a decision by President Obama that it would be fruitless for the government to try to compel the technology companies to provide the keys to protected conversations and data.

Apple has already made encryption technology a standard part of its iMessage service, and Apple's chief executive, Timothy D. Cook, has been among the most vocal in defending a technology for which the keys to decode messages are held not by his company but by the users at each end of the conversation.

Any other approach, Mr. Cook has argued to Mr. Obama, would undercut Apple customers' confidence that the most precious data they keep in their phones is safe from garden-variety cybercriminals as well as sophisticated nation states that could gain access to keys via hacking, or lawfully through court order. Mr. Cook argues that investigators have ways to obtain crucial clues from the available "metadata" about who is talking to whom by phone, from information in the Internet cloud — or, security experts have said, by hacking a target's device.

But the speed of the encryption wave has touched off alarm among law enforcement and intelligence officials, who say it significantly increases the chances that they will miss evidence of an impending attack. Prime Minister David Cameron of Britain threatened late last year to ban such technologies, although he soon backed down. France is threatening to insist on access — and if the French do, so will China, many fear, raising questions about whether the same technology used to crack terrorists' communications will be used to crack dissidents' as well.

"I think this is going to open an entire new debate about security versus privacy," said Michael Morell, a former deputy director of the C.I.A., whose book this year, "The Great War of Our Time," traced the efforts, and failures, in tracking terror plots.

“We have, in a sense, had a public debate” on encryption, he said over the weekend on CBS News’s “Face the Nation.” “That debate was defined by Edward Snowden,” the former National Security Agency contractor who revealed much about the agency’s efforts to break encryption. Now, he said, a new argument will be “defined by what happened in Paris.”

It is also possible the Paris attackers conducted much of their planning face to face, particularly since several lived in the same Brussels neighborhood. But if there was a command center in Syria or elsewhere, some form of communications would have been required.

Just before the Paris attacks, Belgian officials said Islamic State terrorists had been hiding their communication using online gaming tools like Sony’s PlayStation 4 to mask their chatter under that of millions of online video war game players who invoke the same language of violent, religious extremists.

Jan Jambon, Belgium’s federal home affairs minister, told a public audience last week that “PlayStation 4 is even more difficult to keep track of than WhatsApp,” a popular messaging system owned by Facebook.

But if that was the case, it would undermine the argument that end-to-end encryption allowed the Paris terrorism plot to go undetected. While PlayStation and Xbox deploy encryption to protect customers’ personal data like credit card information, it leaves their communications open to government interception in ways that WhatsApp and iMessage do not.

So far, Mr. Obama has been reluctant to insist on a back door into the systems. He rejected the argument of the F.B.I. director, James B. Comey, that the United States should require any company that provides encrypted software and hardware to engineer a way for the government, armed with a court order, to get access. That decision came after a year of study led by the White House counterterrorism adviser, Lisa Monaco, and the head of the White House cybersecurity office, Michael Daniel.

The White House ultimately adopted a view put forth by 14 of the world’s top

cryptographers and computer security experts who wrote, in a white paper, that weakening the encryption of American technology sold by companies like Apple, Google and Facebook would only render confidential data and critical infrastructure more vulnerable to criminals and national adversaries, and push terrorists to adopt encrypted services sold overseas. As a result, when companies like Apple and Facebook are issued court orders to help governments monitor their customers' messages, all they can do is turn over a stream of unintelligible code.

That has inflamed law enforcement officials like Mr. Comey and William J. Bratton, the New York City police commissioner, who told "Face the Nation" on Sunday that encrypting communications in this way had made it impossible for officials to collect warnings on terrorist attacks.

"We, in many respects, have gone blind as a result of the commercialization and the selling of these devices that cannot be accessed either by the manufacturer or, more importantly, by us in law enforcement, even equipped with search warrants and judicial authority," Mr. Bratton said.

Security experts counter that such arguments ignore the fact that even end-to-end encrypted technology leaves a trail of metadata behind that can be used to parse who is talking to whom, when and where. "Encryption is really good at making it difficult to hide the content of communications, but not good at hiding the presence of communications," said Matt Blaze, a computer security expert at the University of Pennsylvania.

Mr. Blaze also noted that the authorities can still read communications if they hack into the target's device, or what security experts call "the end point."

"All the encryption in the world doesn't help if the end point that holds the keys are compromised," Mr. Blaze said. "So this idea that encryption make terrorists' communications go completely dark has a pretty big asterisk next to it."

Even if Apple and others in the United States were compelled to weaken the encryption in their services, American authorities still would have had no judicial authority over Telegram, the Berlin-based messaging service, recently used by

Islamic State terrorists to broadcast their communiqués.

David E. Sanger reported from Washington, and Nicole Perlroth from San Francisco.

Follow the New York Times's politics and Washington coverage on Facebook and Twitter, and sign up for the First Draft politics newsletter.

A version of this article appears in print on November 17, 2015, on page A12 of the New York edition with the headline: Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Attacks.

© 2015 The New York Times Company